National Consumer Protection Week - Dewie's "Hard Shell" on Information Security

Looking for a sign that winter may be coming to an end? February 2 is Groundhog Day, when all eyes are on Punxsutawney Phil, perhaps the world's most famous groundhog, as he looks for his shadow. February 2 is also the start of National Consumer Protection Week, when Dewie, the federal government's information security mascot, will help shed some light on information security practices online. As Phil pops out of his burrow to check the skies, Dewie will be helping consumers find out how to weather viruses and hackers -- or avoid them altogether.

The Federal Trade Commission says NCPW is a great time for the "hard shell" on information security:

1. **Use a strong password.** Hackers may try to steal your passwords to gain access to the personal information stored in your computer. To make it tougher for them, use passwords that have at least eight characters and include numbers or symbols. Avoid common words. Some hackers use programs that can try every word in the dictionary. Don't use your personal information, your login name or adjacent keys on the keyboard as passwords. Don't share your password online or over the phone. Your Internet Service Provider (ISP) should never ask for your password.

2. **Use anti-virus software.** A virus is software that is planted in your computer to damage files and disrupt your system. A virus can result in lost data or require costly repairs to your system. You can avoid these risks by installing and using software that scans your computer and your incoming email for viruses, and then deletes them You can download anti-virus software from the websites of software companies or buy it in retail stores. Look for anti-virus software that recognizes current viruses, as well as older ones; that can effectively reverse the damage; and that updates automatically.

3. **Install a firewall**. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files. A firewall is different from anti-virus protection. Anti-virus software scans your incoming communications and files for troublesome files; a firewall helps make you invisible on the Internet and blocks all communications form unauthorized sources.

4. Back up important files. You can reduce the chances of falling victim to a hacker or virus, but no system is completely secure. If you have important files stored on your computer, copy them onto a removable disk, and store them in a safe place.

5. If your computer is infected, take action immediately. If your computer has been hacked or infected by a virus, disconnect from the Internet right away. Then scan your entire computer with fully updated anti-virus software. Email a report of the incident to your ISP. Often the ISP's email address is abuse@yourispname.com or postmaster@yourispname.com. By doing this, you let the ISP know about the problem on their system and help them plan.

For more information about online security, visit www.ftc.gov/infosecurity.